ДЕСЕТ ПРАКТИЧЕСКИ СТЪПКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

На 25 май тази година влиза в сила Общият регламент относно защитата на данните (GDRP) *(Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година)*, с който се хармонизират правилата за защита на личните данни в държавите-членки.

Общият регламент за защита на данните цели да предостави по-голям контрол на физическите лица относно обработката на личните им данни, да повиши сигурността на данните, както и да предпази субектите, в случаи на нарушения на поверителността или целостта на данните им.

Общият регламент за защита на данните:

Въвежда нови стандарти за съгласието, като правно основание за обработка на данни, укрепва и създава нови права на субектите и предвижда завишени задължения при обработването на данни.

Въвежда нови задължения за работодателите - за отчетност, поддържане на регистри, оценката на риска *и др.*

Създава една общо-приложима рамка – държавите членки не само трябва да го прилагат такъв, какъвто е, без никакви отклонения, но и той ще има абсолютно директно приложение. Т.е. след 25 май 2018 всяко едно физическо лице може да се позове директно на Регламента за защита на личните данни.

1. *ЗАПОЗНАВАНЕ С НОВИТЕ НОРМАТИВНИ ИЗИСКВАНИЯ В ОБЛАСТТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ*

1.1. Определяне на служители или екип, които да отговарят за привеждане на дейността на ДГ/училището – администратор и обработващ

лични данни, в съответствие с новите нормативни изисквания в областта на защитата на личните данни;

1.2. Нормативни документи които трябва да познаваме:

Регламент 2016/679 (Общ регламент относно защитата на данните), Закон за защита на личните данни (ЗЗЛД) и подзаконовите актове по прилагането му, ръководствата и насоките на Комисията за защита на личните данни (КЗЛД) и Работната група по чл. 29 (след 25.05.2018 г. –на Европейския комитет по защита на данните).

2. ВЪТРЕШЕН АНАЛИЗ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

2.1. *Какви категории лични данни и на какви категории физически лица (независимо от тяхното гражданство) се обработват*:

Категории лични данни

• ***„обикновени“ лични данни*** – имена, адрес, електронна поща, IP адрес и т.н.

• ***единен граждански номер***

• ***специални (чувствителни)*** лични данни – данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

Категории физически лица в ДГ/училище на които ще обработваме лични данни

Персонал - педагогически и непедагогически персонал

Деца от 2/3 до 7 години, до постъпването им в 1 клас

Ученици от 1 до 12 клас

Лица навършили 16 години

Родители, Посетители

2.2. За какви конкретни цели се събират, съхраняват и обработват личните данни в ДГ/училище – ***образователен процес, трудови отношения, счетоводство, законово определени цели*** – Наредба № 8/11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование/НЕИСПУО/ и т.н.).

2.3. На кого се предоставят или разкриват личните данни извън ДГ/училището:

• ***на публични органи*** - Национална агенция за приходите, Национален осигурителен институт, Министерство на вътрешните работи, *Министерство на образованието и науката*, съдебни органи, контролни органи, органи на местното самоуправление т.н.

• ***на обработващ лични данни*** (физическо или юридическо лице, което обработва личните данни от името на администратора и по негово нареждане или възлагане)

2.5. Колко време се съхраняват личните данни в ДГ/училището и как е определен този срок –

Наредба № 8/11.08.2016 г. за информацията и документите в системата на ПУО

2.6. Какви мерки за сигурност се прилагат за защита на данните

Прилагане на подходящи технически и организационни мерки за осигуряване на сигурност на данните. В регламента са посочени и конкретни технически и организационни мерки за сигурност, като:

– Псевдонимизация

– Криптиране

– Гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване

– Своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент

3. ОПРЕДЕЛНЕ НА ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

3.1. *Задължение да определи Длъжностно лице по защита на данните* има администратора на лични данни (директорът на ДГ, училището, ЦПЛР):

• ***публичен орган/ДГ, училище, ЦПЛР.../***

3.2. *Определяне на Длъжностно лице по защита на данните* по един от следните алтернативни начини:

• назначаване на служител в ДГ/училище;

• *съвместяване с друга длъжност (без конфликт на интереси);*

• по граждански договор с външно за ДГ/училището/ЦПЛР физическо лице.

3.3. Квалификация на ***длъжностното лице по защита на данните***:

Да има експертни познания в областта на защитата на данните - законодателство и практика – по чл. 28 от Общия регламент за защита на данните

3.4. *Обучение на длъжностното лице по защита на данните:*

• ***първоначално***

• ***текущо***

(Препоръчително е да се определи Длъжностно лице по защита на данните преди да се премине към следващите стъпки.)

4. УПРАВЛЕНИЕ НА РИСКА ПО ОТНОШЕНИЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

4.1. Извършване на оценка на риска на основата на:

• естеството, обхвата, контекста и целите на обработването

• възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест

• последиците за правата и свободите на физическите лица.

4.2. Извършване на оценка на въздействието върху защитата на личните данни при наличие на висок риск (напр. в резултат на профилиране, мащабно обработване на специални (чувствителни) лични данни, систематично мащабно наблюдение на публично достъпна зона, нови технологии и др.).

4.3. Задължителна предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

4.4. Избор на подходящи технически и организационни мерки, за да може да се гарантира и докаже спазване на Регламент 2016/679 и ЗЗЛД. Възможни подходящи мерки могат да бъдат:

• псевдонимизация на личните данни;

• криптиране на личните данни;

• гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

• водене на записи (log files) на дейностите по обработване на данни в системите за автоматизирано обработване;

• *обучение на служители и др.*

4.5. Предприемане на мерки за защита на данните на етапа на проектирането и по подразбиране:

• *на етапа на проектирането*: въвеждане както към момента на определянето на средствата за обработване, така и към момента на самото обработване, на подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на

данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване;

• *по подразбиране*: въвеждане на подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

4.6. Евентуално присъединяване към кодекси за поведение и/ или сертифициране (незадължително).

5. ПРИЕМАНЕ НА ПЛАН ЗА ДЕЙСТВИЕ ЗА ВЪВЕЖДАНЕ НА ОПРЕДЕЛЕНИТЕ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

5.1. Определяне на отговорник и екип.

5.2. Определяне на срокове и етапи за изпълнение.

5.3. Осигуряване на необходими финансови, технически и човешки ресурси.

6. ПРЕГЛЕД НА ПРАВНИТЕ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ, ВКЛЮЧИТЕЛНО ВЪЗ ОСНОВА НА СЪГЛАСИЕ НА ЛИЦАТА

6.1. Преглед на използваните до момента алтернативни правни основания за обработване на лични данни:

• *съгласие –Условия за даване на съгласие по чл. 7*

Условия, приложими за съгласие на дете във връзка с услугите на информационното общество по чл. 8 от Общия регламент

• сключване или изпълнение на договор

• *законово задължение за администратора*

• защита на жизненоважни интереси на субекта на данните или на друго физическо лице

• изпълнение на задача от обществен интерес или упражняването на официални правомощия, предоставени на администратора

6.2. Преценка дали е законосъобразно и целесъобразно обработването на лични данни - да е на основание единствено съгласието на лицето. В този случай администраторът следва да е в състояние да докаже, че съгласието е:

• *свободно изразено* – не дадено под натиск или заплаха от неблагоприятни последици (напр. по-висока цена на услуга);

• *конкретно* – отделно съгласие за всяка конкретно определена цел, а когато е относимо и за конкретна категория лични данни;

• *информирано* – дадено на основата на пълна, точна и лесно разбираема информация;

• *недвусмислено* – не се извлича или предполага на основата на други изявления или действия на лицето;

• ***изрично изявление или ясно потвърждаващо действие – мълчанието на лицето вече не може да се приеме за съгласие.***

6.3. Документиране на съгласието с цел доказване пред Комисията за защита на личните данни и съда (декларации и др.).

6.4. Осигуряване на практическа възможност на субекта на данните да оттегли по всяко време съгласието си толкова лесно, колкото го е дал.

6.5. *В случай на пряко предлагане на услуги на информационното общество на дете под 16 години - избор на процедура и/ или технология за удостоверяване, че съгласието е дадено или разрешено от носещия родителска отговорност за детето. (Когато е налице правно основание за обработване на лични данни, различно от съгласието, напр. нормативно*

задължение или договор, администраторът не следва да дублира това основание и със съгласие на лицето).

7. ИНФОРМИРАНОСТ НА СУБЕКТИТЕ НА ДАННИТЕ И ПРОЗРАЧНОСТ НА ОБРАБОТВАНЕТО

7.1. Предоставяне на обобщена, кратка и разбираема информация чрез интернет сайта на ДГ/училището/ЦПЛР или по друг достъпен за субектите на данни начин относно:

• идентифициране на ДГ/училището – наименование и начин за контакт, включително с *Длъжностното лице по защита на данните* (адрес, електронна поща, телефон и т.н.)

• какви категории лични данни се събират и за какви цели се обработват

• срока за съхранение на данните

• съществуването на конкретни права на субектите на данните (право на достъп, коригиране или изтриване на лични данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните) и реда за упражняването им

• правото на субектите на данни да подадат жалба до КЗЛД или до съда

• дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени

7.2. Информиране по подходящ начин на педагогическия и непедагогически персонал, на децата, учениците и техните родители, лицата навършили 16 години, продължаващи образованието си, в случай, че:

• се извършва видеонаблюдение в ДГ/училището/ЦПЛР;

• следи средствата за електронна комуникация на работното място, предоставени от ДГ/училището (интернет, телефон, мобилен телефон), с цел предотвратяване на злоупотреби.

8. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

8.1. Познаване от страна на администратора и неговите служители на правата, които Регламент 2016/679 предоставя на лицата право на достъп до личните данни, свързани с лицето, които се обработват от ДГ/училището

• право на коригиране или допълване на неточни или непълни лични данни

• право на изтриване („право да бъдеш забравен“) на лични данни, които се обработват незаконосъобразно или с отпаднало правно основание (изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани и др.)

• право на ограничаване на обработването - при наличие на правен спор...

• право на преносимост на данните – ако се обработват по автоматизиран начин на основание съгласие или договор

• право на възражение - по всяко време и на основания, свързани с конкретната ситуация на лицето, при условие, че не съществуват убедителни законови основания за обработването...

8.2. *Разписване на вътрешни процедури за приемане, разглеждане и отговаряне в едномесечен срок на искания от физически лица за упражняване на правата им като субекти на лични данни и създаване на организация за прилагането им на практика*

9. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

9.1. Приемане на вътрешна процедура и/или план за действие в случай на нарушение на сигурността на личните данни.

9.2. Определяне на отговорен служител/екип за реакция при нарушение на сигурността на личните данни, инструктаж на персонала, др.

9.3. Създаване на вътрешна организация за своевременно уведомяване на КЗЛД в срок до 72 часа от узнаването за нарушението.

10. ДОКУМЕНТИРАНЕ И ОТЧЕТНОСТ

В съответствие с принципа на *отчетност* всеки администратор е длъжен:

- да прилага на практика принципите за защита на личните данни, съгласно Регламент 2016/679

и

- да удостовери и докаже, че обработването на лични данни съответства на тези принципи.

Дейностите по документиране и отчетност обхващат, като минимум, следните мерки и стъпки:

10.1. Създаване и редовно актуализиране на вътрешен регистър на дейностите по обработване на лични данни в ДГ/училището/ЦПЛР със следната информация:

• името и координатите за връзка на *администратора* и, когато това е приложимо, на *длъжностното лице по защита на данните*, ако има такива;

• целите на обработването;

• описание на категориите субекти на данни и на категориите лични данни;

• категориите получатели, пред които са или ще бъдат разкрити личните данни;

• предвидените срокове за изтриване на различните категории данни;

• общо описание на техническите и организационни мерки за сигурност.

10.2. Приемане на вътрешна инструкция/правила/процедури/ политика за защита на личните данни в ДГ/училище/ЦПЛР

10.3. План за действие за въвеждане на технически и организационни мерки

10.4. Други – заповеди, декларации, заявления.....